recharge a power-supply of the device is disabled. The device protection method **350** ends following the disabling (**366**) of the recharger.

[**0033**] FIG. **4**A depicts a guardian **400** provided for protection of one or more devices **402** and **404** in accordance with one embodiment of the invention. Guardian **400** can, for example, be provided in computing system (e.g., a server) **410** that provides one or more services accessible via devices **402** and **404**. In general, devices **402** and **404** can communicate with the computing system **410**. Typically, the connection is initiated by the device **402** or **404** in order to receive a service (e.g., download music, play movies, access accounts).

[**0034**] When a connection is established between a device **402** (or device **404**) and the computing system **410** and/or another computing system **412** that is monitored by the computing system **410**, the guardian **400** may be activated. When activated, the guardian **400** determines whether there is potential unauthorized use of the device **402** (or device **404**). More particularly, the guardian **400** can access a database **420** to determine what to check and what action to take for a particular device. By way of example, when device **402** makes a connection to the computing system **410** in order to access a service (e.g., download music), the guardian **400** can determine the identifier assigned to the device **402** and look it up in the database **420**. The information stored in the database **420** for the specific device **402** (or device category of devices) can, for example, indicate that if a download is requested, verify that the device has not been reported stolen, an/or verify that device **402** is within a geographical location, and so on. Depending on the result of the verification process, one or more actions may be taken. By way of example, the recharger of device **402** may be disabled and/or the requested operation may be denied.

[**0035**] FIG. **5** depicts a monitoring method **500** for monitoring activities of devices in accordance with one embodiment of the invention. Initially, it is determined (**502**) whether a connection is established with a device. A connection can, for example, be initiated by the device to an entity (e.g., server) designated to monitor devices. In any case, if it is determined (**502**) that a connection is established with the device, it is determined (**504**) whether unauthorized use of the device is suspected (e.g., the device is reported as stolen, device is out of the designated area). If it is determined (**504**) that unauthorized use is not suspected, it is determined (**502**) whether a connection is established with the device. In other words, a first connection established with the device is effectively ignored when it is determined (**504**) that unauthorized use of the device is not suspected. However, if it is determined (**504**) that unauthorized use of the device is suspected, it is determined (**506**) whether the use is authorized. By way of example, a security-code can be requested, entered, and compared with the one which is assigned to that particular device. If it is determined (**506**) that the use of device is authorized, the connection is effectively ignored and/or the device is allowed to receive services (e.g., download music) or perform operations. On the other hand, if it is determined (**506**) that the device has not been authorized, one or more actions can be performed (**508**) in response to the suspected unauthorized use (e.g., the recharge-circuit for the device may be disabled by sending a disable command and/or installing firmware, downloading capabilities of the device can be disabled by installing firmware or software on the device). The device monitoring method **500** ends after one or more operations are performed (**508**) in response to suspicion of unauthorized use of the device.

What is claimed is:

1. A method for guarding against unauthorized use of a device, said method comprising:

determining whether to disable a recharger associated with said device in order to protect said device against unauthorized use of said device, wherein said device can be powered by a rechargeable-power-supply that can be charged by said recharger when said recharger is enabled; and

disabling said recharger associated with said device so that said rechargeable-power-supply cannot be charged by said recharger.

2. A method as recited in claim 1, wherein said disabling of said rechrager effectively renders said device inoperable when the rechargeable-power-supply runs out of power.

3. A method as recited in claim 1, wherein said rechargeable-power-supply is the main power supply for said device.

4. A method as recited in claim 3,

wherein said device is a handheld-device, and

wherein said rechargeable-power-supply is the main power supply for said device.

5. A method as recited in claim 1, wherein said device is one or more of the following:

a personal computer, a cell phone, a Global Positioning System (GPS), a media-player, a wireless device, a handheld-device, a personal digital assistant, a music-player.

6. A method for protecting a device against unauthorized use, said method comprising:

determining whether unauthorized use of said device can be suspected; and

disabling a recharger associated with said device so that a rechargeable-power-supply that normally powers said device cannot be charged by said recharger.

7. A method as recited in claim 6, wherein said determining of whether unauthorized use of said device can be suspected comprises:

determining whether an event, condition, or situation indicates that said device may be in use without authorization.

8. A method as recited in claim 6, wherein said determining of whether unauthorized use of said device can be suspected comprises one or more of the following:

determining whether said device has been connected to another object;

determining whether said device is out of a determined geographical boundary; and

determining whether a timer has expired.

9. A method as recited in claim 8, wherein said object is one or more of the following: another device, an adaptor that connects said device to a power-supply, a server, a personal computer.

10. A method as recited in claim 6, wherein said method further comprises: